Engineering Principles for IT Security

(A baseline for achieving security)

Recommendations of the
National Institute of Standards and Technology

Draft

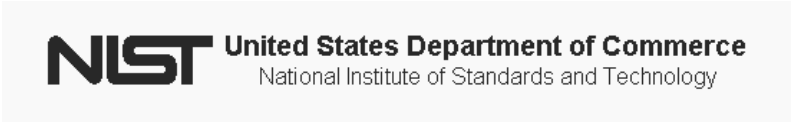

TABLE OF CONTENTS

1.0 INTRODUCTION

1.1 Authority

This document has been developed by NIST in furtherance of its statutory responsibilities (under the Computer Security Act of 1987 and the Information Technology Management Reform Act of 1996, specifically 15 U.S.C. 278 g-3(a)(5)). This is not a guideline within the meaning of (15 U.S.C. 278 g-3 (a)(3)).

These guidelines are for use by Federal organizations which process sensitive information.1 They are consistent with the requirements of OMB Circular A-130, Appendix III.

The guidelines herein are not mandatory and binding standards. This document may be used by non-governmental organizations on a voluntary basis. It is not subject to copyright.

Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding upon Federal agencies by the Secretary of Commerce under his statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, the Director of the Office of Management and Budget, or any other Federal official.

1.2 Purpose

> **Principle *n.*** – A rule or standard, especially of good behavior.
>
> American Heritage Dictionary

The purpose of the Engineering Principles for Information Technology (IT) Security (EP-ITS) is to present a list of system-level security principles to be considered in the design, development, and operation of an information system.

Ideally, the principles explained here would be used from the onset of a program—at the beginning, or during the design phase—and then employed throughout the system's life-cycle. However, these principles are also helpful in affirming and confirming the security posture of already deployed information systems. The principles are short and concise and can be used by organizations to develop their system life cycle policies.

1 Many people think that sensitive information only requires protection from unauthorized disclosure. However, the Computer Security Act provides a much broader definition of the term "sensitive information:" *any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy*.

1.3 Scope

This document is published by the National Institute of Standards and Technology (NIST) as recommended guidance for Federal departments and agencies and is intended to be used by both the government and private sector.

This document should be used by those interested in IT security and the principles introduced should be applied to general support systems and major applications.

This document presents principles, not solutions, at a fairly generic level. Said another way, the goal is to present principles that apply to all systems, not ones tied to specific technology areas. The latter would be accomplished by use of this document in developing more detailed guidance.

1.4 Audience

The intent is to provide IT security principles that interested parties can use in securing a given information system. For example, these principles can be used by:

- **Users** when developing and evaluating functional requirements, or when operating information systems within their organizations.
- **System Engineers and Architects** when designing, implementing, or modifying an information system.
- **IT Specialists**[2] during all phases of the system lifecycle.
- **Program Managers and Information System Security Officers (ISSO)** to ensure adequate security measures have been considered for all phases of the system life-cycle.

1.5 Document Structure

Section 1 of this document provided the purpose and scope, and makes clear this document audience. Section 2 provides background information, including how this document is related to other NIST, Federal, and international documents and initiatives including *Generally Accepted Principles and Practices for Securing Information Technology Systems*, SP 800-14, September 1996, and the Common Criteria. Section 3, the main section of this document, presents 32 security principles and identifies their applicability in the life-cycle phases. Section 4 is a short summary. This document also has three appendices; Appendix A provides background on the new OPM IT specialist sub-categories. It also contains a table that identifies when in the system lifecycle they might be most involved with security. Appendix B defines terms throughout this document and Appendix C provides a list of referenced documents.

[2] *IT Specialist* is a new occupation title created by the Office of Personnel Management (OPM) under the Information Technology Management series. Within this occupation OPM has identified several specialty areas referred to as "parenthetical titles." In this document we use the generic term throughout but have provided additional detail in Appendix A.

2.0 BACKGROUND

Private businesses and government agencies, both foreign and domestic, are becoming increasingly reliant on information technology to fulfill many basic functions. Businesses are making changes simply to remain competitive in the changing global marketplace. Likewise, government agencies are seeking to provide better service to their citizens.

Regardless of the reason, the move to a digital economy has caused information and information technology to become valuable business assets that need to be protected. With this development has come the recognition that fulfilling these basic functions requires as a matter of course comprehensive, well-designed, and reliable information system security programs.

Significant information system security program standards, guidance, and implementation strategies have been, or are being, developed by public and private sector organizations in the United States and abroad. These wide-ranging efforts are designed to address many aspects of information security at many levels of detail. They address specific topics such as public key infrastructure (PKI) and certification and accreditation (C&A) processes, and more general topics such as organizational best practices.

Seeking to support and guide these many efforts, several private and public organizations have developed a number of explicit and implicit information system security principles. These security principles, in turn, have formed an extensive canon for users, designers, and engineers to consider in designing information system security programs.

This document seeks to compile and present many of these security principles into one, easy-to-use document for those concerned with information system security. But, in contrast to other organization-level efforts, the principles in this document are structured around a system-level, engineering approach.

2.1 *Generally Accepted Principles and Practices for Securing Information Technology Systems* (SP 800-14)

SP 800-14 provides a foundation upon which organizations can establish and review information technology security programs. The document is designed to be used by all levels of management and by those responsible for computer security at the organization and system-level. The eight Generally Accepted System Security Principles in SP 800-14 are designed specifically to provide the public or private sector audience an organization-level perspective when creating new systems, practices, or policies.

The principles in this document provide a system-level, perspective for information technology security. These principles are derived primarily from concepts found in the eight principles and 14 practices identified in the SP 800-14.

It should be noted the principles in this document are not ordered under that same headings used in SP 800-14. This is due to the different focus for the two documents and is akin to the loose relationship between principles and practices that exists in SP 800-14.

2.2 Common Criteria

The Common Criteria (CC) methodology is a repeatable method of documenting IT security requirements, documenting and validating product security capabilities, and promoting international cooperation in the area of IT security.

Use of Common Criteria "protection profiles" and "security targets" greatly aids the development of products or systems that have IT security functions. The rigor and repeatability of the Common Criteria yields the thorough definition of user security needs needed by developers. Validated security targets provide system integrators with key information needed in the procurement security components and implementation of secure IT. The approach of this document meshes with the methodology of the Common Criteria.

2.3 Defense-in-Depth

The need for securing information and systems against the full spectrum of threats dictates the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information technology. This fundamental need for layered protections is captured in the “Defense-in-Depth” strategy being used by DoD for protecting information systems, both classified and unclassified.

This strategy recognizes that due to the highly interactive nature of the various systems and networks, any single system cannot be secured adequately unless all interconnecting systems are also secured adequately. This strategy calls for use of multiple, overlapping protection approaches to ensure the failure or circumvention of any individual protection approach will not leave the system unprotected. Through user training and awareness, well-crafted policies and procedures, and redundancy of protection mechanisms, the “Defense-in-Depth” strategy enables the people, operations, and technology to ensure effective protection of information technology so that mission objectives can be confidently achieved.

One source of information on implementing the “Defense-in-Depth” strategy is the Information Assurance Technical Framework (IATF). The IATF advocates the use of multiple information technology protection methods or approaches following the “Defense-in-Depth” strategy to establish a composite security posture adequate to blunt threats.

The principles and technical guidance in this document are consistent with the DoD’s “Defense-in-Depth” strategy. For more information on “Defense-in-Depth,” please refer to the Department of Defense Chief Information Officer Guidance and Policy Memorandum No, 6-8510, “Department of Defense Global Information Grid Information Assurance,” which can be found on the world-wide web at http://www.c3i.osd.mil/org/cio/doc/gigia061600.pdf.

3.0 SECURITY PRINCIPLES

3.1 Introduction

To aid in designing a secure information system, NIST compiled a set of engineering principles for system security. These principles provide a foundation upon which a more consistent and structured approach to the design, development, and implementation of IT security capabilities can be constructed.

While the primary focus of these principles remains on the implementation of technical countermeasures, these principles highlight the fact that, to be effective, a system security design should also consider non-technical issues, such as policy, operational procedures, and user education.

The principles described here do not apply to all systems at all times—each principle should be carefully considered throughout the system life cycle. Moreover, because of the constantly changing information system security environment, the principles identified are not considered to be an inclusive list. Instead, this document is an attempt to present in a logical fashion fundamental security principles that can be used in today's operational environments. As technology improves and security techniques are refined, additions, deletions, and refinement of these security principles will be required.

Each principle has two components. The first is a table that indicates where the principle should be applied during the system life cycle. The second is an explanatory narrative further amplifying the principle.

The five life-cycle planning phases used are defined in the *Generally Accepted Principles and Practices for Securing Information Technology Systems*, SP 800-14:

- Initiation Phase
- Development/Acquisition Phase
- Implementation Phase
- Operation/Maintenance Phase
- Disposal Phase.

In an effort to associate each principle with the relevant life-cycle planning phase(s), a table similar to the example table below, Table 3-1, has been developed for each principle. The table identifies each life-cycle phase and "check marks" are used to indicate if the principle should be considered or applied during the specified phase. One check "✔" signifies the principle can be used to support the life-cycle phase and two checks "✔✔" signifies the principle is key to successful completion of the life-cycle phase.

TABLE 3-1 EXAMPLE LIFE-CYCLE APPLICABILITY TABLE

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability	✔✔	✔		✔	

For example, the table above indicates that Principle No. X *must* be considered and is key to the successful completion of the Initiation phase. Additionally, Principle No. X, *should* be considered and applied in support of the Development/Acquisition and the Operation/Maintenance phases.

3.2 System Life Cycle Description

The following brief descriptions of each of the five phases of the system lifecycle are taken from *Generally Accepted Principles and Practices for Securing Information Technology Systems*, SP 800-14.

- **Initiation:** During the initiation phase, the need for a system is expressed and the purpose of the system is documented. Activities include conducting a sensitivity assessment.
- **Development/Acquisition:** During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle. Activities include determining security requirements, incorporating security requirements into specifications, and obtaining the system.
- **Implementation:** During implementation, the system is tested and installed or fielded. Activities include installing/turning on controls, security testing, and accreditation.
- **Operation/Maintenance:** During this phase, the system performs its work. The system is almost always being continuously modified by the addition of hardware and software and by numerous other events. Activities include security operations and administration, operational assurance, and audits and monitoring.
- **Disposal:** The disposal phase of the IT system life cycle involves the disposition of information, hardware, and software. Activities include moving, archiving, discarding or destroying information and sanitizing the media.

3.3 IT Security Principles

Principle 1.	*Establish a sound security policy as the "foundation" for design.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability	✔✔	✔	✔	✔	

Discussion: A security policy is an important document to develop while designing an information system. The security policy begins with the organization's basic commitment to information security formulated as a general policy statement. The policy is then applied to all aspects of the system design or security solution. The policy identifies security goals (e.g., confidentiality, integrity, availability, accountability, and assurance) the system should support,

and these goals guide the procedures, standards and countermeasures used in the IT security architecture design.

Principle 2.	*Clearly delineate the physical and logical security boundaries governed by associated security policies.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability	✔✔	✔✔	✔	✔	

Discussion: Information technology exists in physical and logical locations, and boundaries exist between these locations. An understanding of what is to be protected from external factors can help ensure adequate protective measures are applied where they will be most effective. Sometimes a boundary is defined by people, information, and information technology associated with one physical location. But this ignores the reality that, within a single location, many different security policies may be in place, some covering publicly accessible information and some covering sensitive unclassified information. Other times a boundary is defined by a security policy that governs a specific set of information and information technology that can cross physical boundaries. Further complicating the matter is that, many times, a single machine or server may house both public-access and sensitive unclassified information. As a result, multiple security policies may apply to a single machine or within a single system. Therefore, when developing an information system, security boundaries must be considered and communicated in relevant system documentation and security policies.

Principle 3.	*Reduce risk to an acceptable level.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability	✔✔	✔✔	✔✔	✔✔	✔✔

Discussion: Previously, risk avoidance was a common IT security goal. That changed as the nature of the risk became better understood. Today, it is recognized that elimination of all risk is not cost-effective. A cost-benefit analysis should be conducted for each proposed countermeasure. In some cases, the benefits of a more secure system may not justify the direct and indirect costs. Direct costs include the cost of purchasing and installing a given technology; indirect costs include decreased system performance and additional training. The goal is to enhance mission/business capabilities by managing mission/business risk to an acceptable level.

Principle 4.	*Assume that external systems are insecure.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability	✔✔	✔✔	✔	✔✔	✔

Discussion: The term information domain arises from the practice of partitioning information resources according to access control, need, and levels of protection required. Organizations implement specific measures to enforce this partitioning and to provide for the deliberate flow of authorized information between information domains. An external domain is one that is not under your control.

In general, external systems should be considered insecure. A threat analysis should be conducted on the external system to determine the range of unknown threat-sources. Until an external domain has been deemed "trusted," system engineers, architects, and IT specialists should presume the security measures of an external system are different than those of a trusted internal system and design the system security features accordingly.

Principle 5.	*Identify potential trade-offs between reducing risk, i.e., increasing assurance, and increased costs and decreased operational effectiveness.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability	✔✔	✔✔		✔✔	

Discussion: To meet stated security requirements, a systems designer, architect, or security practitioner will need to identify and address all competing operational and security concepts. It may be necessary to modify or adjust security principles and goals to meet stated operational requirements. In modifying or adjusting security principles, an acceptance of greater risk and cost may be inevitable. By identifying and addressing these trade-offs as early as possible, decision makers will have greater latitude and the negative aspects of the trade-space can be minimized.

Principle 6.	*Ensure no single point of failure.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔✔	✔	✔✔	✔

Discussion: Security designs should consider a layered approach to address or protect against a specific threat or to reduce a vulnerability. For example, the use of a packet-filtering router in conjunction with an application gateway and an intrusion detection system combine to increase the work-factor an attacker must expend to successfully attack the system. Adding good password controls and adequate user training improves the system's security posture even more.

Principle 7.	*Implement tailored system security measures to meet organizational security goals.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔✔	✔	✔✔	✔

Discussion: In general, IT security measures are tailored according to an organization's unique needs. While numerous factors, such as the overriding mission requirements, and guidance, are to be considered, the fundamental issue is the protection of the mission or business from IT security-related, negative impacts. Because IT security needs are not uniform, system designers and security practitioners should consider the level of trust when connecting to other external networks and internal sub-domains. Recognizing the uniqueness of each system allows a layered security strategy to be used–implementing lower assurance solutions with lower costs to protect less critical systems and higher assurance solutions only at the most critical areas.

Principle 8.	*Design and implement security measures to be proportional to the program risks and mission impact.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability	✔	✔✔	✔	✔	✔

Discussion: Security controls should be designed based on risk. Risk to the system can be defined as he probability that a particular threat source will exploit, or trigger, a particular information system vulnerability. Security controls implemented to counter this risk should be designed in proportion to the risk so that the organization's goals and objectives are supported and enhanced. Security controls should not be designed to hinder the pursuit of the organization's goals and objectives.

Principle 9.	*Strive for simplicity.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔✔	✔	✔✔	

Discussion: The more complex the mechanism, the more likely it may possess exploitable flaws. Further, simple mechanisms tend to have fewer exploitable flaws and require less maintenance. Finally, because configuration management issues are simplified, updating or replacing a simple mechanism becomes a less intensive process.

Principle 10.	*Design and operate an IT system to prevent vulnerability and to be resilient in response.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔✔		✔✔	

Discussion: Information systems should be resistant to attack, should limit damage, and should recover rapidly when attacks do occur. This is especially true for systems built using current, state-of-the-art COTS products. The principle suggested here recognizes the need for adequate protection technologies at all levels to ensure that any potential cyber attack will be countered effectively. There are vulnerabilities that cannot be fixed, those that have not yet been fixed, those that are not known, and those that could be fixed but are not (e.g., risky services allowed through firewalls) to allow increased operational capabilities. In addition to achieving a secure initial state, secure systems should have a well-defined status after failure, either to a secure failure state or via a recovery procedure to a known secure state. Organizations should establish detect and respond capabilities, manage single points of failure in their systems, and implement a reporting strategy.

Principle 11.	*Treat security as an integral part of the overall system design.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability	✔	✔✔	✔	✔✔	✔

Discussion: Security must be considered in information system design. Experience has shown it is very difficult to implement security measures properly and successfully after a system has been developed, so it should be integrated fully into the system life-cycle process. This includes understanding the security requirements, participating in the evaluation of security products, and finally in the engineering, design, and implementation, and disposal of the system.

Principle 12.	*Minimize the system elements to be trusted.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔✔	✔	✔✔	

Discussion: To achieve a maintainable protection level, security measures should be as simple as possible. Security measures include people, operations, and technology. If technology is used, hardware, firmware, and software should be designed and implemented so that other system elements need not be trusted to maintain protection. Further, to ensure cost-effective and timely certification of system security features, it is important to minimize the amount of software and hardware expected to provide the most secure functions for the system.

Principle 13.	*Implement security through a combination of measures distributed physically and logically.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔✔	✔	✔	✔

Discussion: Often, a single security service is achieved by cooperating elements existing on separate machines. For example, a system authentication is typically accomplished using elements ranging from the user-interface on a workstation through the networking elements to an application on an authentication server. It is important to associate all elements with the security service they provide. These components are likely to be shared across systems to achieve security as infrastructure resources come under more senior budget and operational control. Proper disposal mechanisms for system elements, especially media, during operations and disposal phase is critical to maintenance of confidentiality.

Principle 14.	*Provide assurance that the system is, and continues to be, resilient in the face of expected threats.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔✔	✔	✔✔	✔

Discussion: Assurance is the grounds for confidence that a system meets its security expectations. These expectations can typically be summarized as - providing sufficient resistance to both direct penetration and attempts to circumvent security controls. Good understanding of the threat environment, evaluation of requirement sets, hardware and software engineering disciplines, and product and system evaluations are primary measures used to achieve assurance. Additionally, the documentation of the specific and evolving threats is important in making timely adjustments in applied security and strategically supporting incremental security enhancements.

Principle 15.	*Isolate system elements to limit or contain vulnerabilities.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔✔	✔	✔	

Discussion: To limit or contain vulnerabilities, system elements should be isolated from each other. If a vulnerability does exist in an information domain, damage can be limited or contained to this domain, allowing other information system domains to function properly. Limiting and containing insecurities also helps to focus response and reconstitution efforts to information system areas most in need.

Principle 16.	*Formulate security measures to address multiple overlapping information domains.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability	✔	✔✔	✔	✔	

Discussion: An efficient and cost effective security capability should be able to enforce multiple security policies to protect successfully multiple information domains without the need to separate physically the information and respective information systems processing the data. This principle argues for moving away from the traditional practice of creating separate LANs and infrastructures for various sensitivity levels and moving toward solutions that enable the use of common, shared, public infrastructures with appropriate protections at the operating system, application, and workstation level.

Moreover, to accomplish missions and protect critical functions, government and private sector organizations have many types of information to safeguard. With this principle in mind, system engineers, architects, and IT specialists should develop a security capability that allows organizations with multiple levels of information sensitivity to achieve the basic security goals in an efficient manner.

Principle 17.	*Isolate public access systems from mission critical resources (e.g., data, processes, etc).*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability	✔	✔✔	✔	✔	

Discussion: While the trend toward shared infrastructure has considerable merit in almost all cases, it is not universally applicable. In cases where the sensitivity or criticality of the information is high, organizations may want to limit the number of systems on which that data is stored and isolate them, either physically or logically. Physical isolation may include ensuring that no physical connection exists between an organization's public access information resources and an organization's critical information. When implementing logical isolation solutions, layers of security services and mechanisms should be established between public systems and secure systems responsible for protecting mission critical resources. Security layers may include using network architecture designs such as demilitarized zones and screened subnets. Finally, system designers and administrators should enforce organizational security policies and procedures regarding use of public access systems.

Principle 18.	*Use boundary mechanisms to separate computing systems and network infrastructures.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔✔	✔	✔✔	

Discussion: To control the flow of information and access across network boundaries in computing and communications infrastructures, and to enforce the proper separation of user groups, a suite of access control devices and accompanying access control policies should be used. A combination of routers, firewalls and intrusion detection mechanisms to monitor access can offer reasonable protection. High assurance gateways and one way transfer mechanisms offer higher assurance of separation, but typically at greater acquisition and management costs.

Principle 19.	*Where possible, base security on open standards for portability and interoperability.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability	✔	✔✔			

Discussion: Most organizations depend significantly on distributed information systems to perform their mission or business. These systems distribute information across their own organization and also with other external organizations. For security capabilities to be effective in such environments, security program designers should make every effort to incorporate interoperability into all security measures, including hardware and software, and implementation practices.

Principle 20.	*Implement and employ layered protections to mitigate vulnerabilities in COTS products.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔✔	✔	✔✔	

Discussion: Practical experience has shown that even with the current state-of-the-art for security quality in COTS, a high degree of protection against sophisticated attacks is not guaranteed. It is possible to mitigate this situation by placing several countermeasures in series, requiring additional work by attackers to accomplish their goals. This principle is closely related to others above, yet is stated due to the inherent weaknesses of COTS and the need to explicitly address these weaknesses in the design and architecture.

Principle 21.	*Use common language in developing security requirements.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability	✔✔	✔✔		✔✔	

Discussion: The use of a common language when developing security requirements permits organizations to evaluate and compare security products and features evaluated in a common test environment. When a "common" evaluation process is based upon common requirements or criteria, a level of confidence can be established that ensures product security functions conform to an organization's security requirements. A good source for this methodology is the Common Criteria.

Principle 22.	*Design and implement audit mechanisms to detect unauthorized use and to support incident investigations.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔✔	✔✔	✔	

Discussion: Organizations should monitor, record, and review periodically audit logs to identify unauthorized use and to ensure system resources are functioning properly. In some cases, organizations may be required to disclose information obtained through auditing mechanisms to appropriate third parties, including law enforcement authorities or Freedom of Information Act (FOIA) applicants. Many organizations have implemented consent to monitor policies which state that evidence of unauthorized use (e.g., audit trails), may be used to support administrative or criminal investigations..

Principle 23.	*Design security to allow for regular adoption of new technology, including a secure and logical technology upgrade process.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔✔	✔	✔✔	

Discussion: As mission and business processes change, security requirements and technical protection methods must be updated. IT-related risks to the mission/business vary over time and undergo periodic assessment. Periodic assessment should be performed to enable system designers and managers to make informed risk management decisions on whether to accept or mitigate identified risks with changes or updates to the security capability. The lack of timely identification through consistent security solution re-evaluation and correction of evolving, applicable IT vulnerability flaws results in false trust and increased flaw exploitation opportunities.

Each security mechanism should be able to support migration to new technology or upgrade of new features without requiring an entire system redesign. The security design should be modular so that individual parts of the security design can be upgraded without the requirement to modify the entire system. Although this is a goal, the struggle to achieve this ultimately results in a debate of COTS vendor product alignments versus self-maintained interface code.

Principle 24.	*Authenticate users and processes to ensure appropriate access control decisions are made across domains.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔	✔	✔✔	✔

Discussion: Level of trust is always an issue when dealing with cross-domain interactions. The solution is to establish an authentication policy and apply it to cross-domain interactions as required. Authentication is the process where a system establishes the validity of a transmission, message, or a means of verifying the eligibility of an individual, process, or machine to carry out a desired action, thereby ensuring that security is not compromised by an untrusted source. Note: A user may have rights to use more than one name in multiple domains. Further, rights may differ among the domains, potentially leading to security policy violations.

Principle 25.	*Use unique identities to ensure accountability.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔	✔	✔✔	

Discussion: An identity may represent an actual user, a process with its own identity, e.g., a program making a remote access, or a number of users represented by single identity, e.g., a role. Unique identities are required:

- To maintain accountability and traceability of a user or process
- To assign specific rights to an individual user or process
- To provide for non-repudiation
- To enforce access control decisions
- To establish the identity of a peer in a secure communications path
- To prevent unauthorized users from masquerading as an authorized user.

Principle 26.	*Use roles to control user and process access.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔	✔	✔✔	

Discussion: The system security policy should clearly identify and define the various roles of users or processes. Once identified or defined, each role is assigned well-defined permissions needed to perform its functions. Each permission specifies a permitted access to a particular resource (such as "read" and "write" access to a specified file or directory, "connect" access to a given host and port, etc.). Unless a permission is granted explicitly, the user or process should not be able to access the protected resource.

This concept of limiting access, or "least privilege," is most often applied in the administration of the system. Its goal is to reduce risk by limiting the number of people with access to critical system security controls; i.e., controlling who is allowed to enable or disable system security features or change the privileges of users or programs. Best practice suggests it is better to have several administrators with limited access to security resources rather than have one person with "super user" permissions. A high level of trust should be placed on a "super user" since they have the ultimate power to control or destroy an organization's information.

Principle 27.	*Maintain traceability from security goals and requirements to security mechanisms.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability	✔	✔✔		✔✔	

Discussion: Every security mechanisms should support a security service or set of services, and every security service should support one or more security goals. Extra measures should not be implemented if they do not support a recognized service or security goal. Such mechanisms could add unneeded complexity to the system and are potential sources of additional vulnerabilities.

An example is file encryption supporting the access control service that in turn supports the goals of confidentiality and integrity by preventing unauthorized file access. If file encryption is a necessary part of accomplishing the goals, then the mechanism is appropriate. However, if these security goals are adequately supported without inclusion of file encryption, then that mechanism would be an unneeded system complexity.

Principle 28.	*Ensure the integrity, confidentiality, and availability of information being processed, in transit, and in storage.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔✔	✔	✔✔	✔

Discussion: The risk of unauthorized modification or destruction of data, disclosure of information, and denial of access to data while in transit should be considered along with the risks associated with data that is in storage or being processed. Therefore, system engineers, architects, and IT specialists should implement security measures to preserve the integrity, confidentiality, and availability of data, including application software, while the information is being processed, in transmit, and in storage.

Principle 29.	*Strive for operational ease of use*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔✔	✔	✔✔	

Discussion: A security measure difficult to maintain and keep in an operational state is not effective; it should enhance the organization's mission and business operation. The experience and expertise of administrators and users should be appropriate and proportional to the operation of the security measure. If this is not the case, then an organization must invest resources to ensure system administrators and users are properly trained. Moreover, administrator and user training costs along with the life-cycle operational costs should be considered when determining whether the security measure is a viable one.

Principle 30.	*Develop and exercise contingency or disaster recovery procedures to ensure appropriate availability.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability	✔	✔	✔	✔✔	

Discussion: Continuity of operations plans or disaster recovery procedures address continuance of an organization's operation in the event of a disaster or prolonged service interruption that affects the organization's information system and security capability. Such plans should address an emergency response phase, a recovery phase, and a return to normal operation phase. Personnel responsibilities during an incident and available resources should be identified. In reality, contingency and disaster recovery plans do not address every possible scenario or assumption. Rather, it focuses on the events most likely to occur and identifies an acceptable method of recovery. Periodically, the plans and procedures should be exercised to ensure that they are effective and well-understood.

Principle 31.	*Consider custom products to achieve adequate security.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔✔	✔	✔	

Discussion: To provide security services, comprehensive use of COTS products by security program designers may not be possible in some legacy systems. To provide theses service, the system security designer should analyze and understand the risk presented by the non-COTS security products. Once these risks are measured, security designers can mitigate the risks by designing a security mechanism that uses the non-COTS products of the legacy system augmented by selected applications of COTS products.

Principle 32.	*Ensure proper security in the shutdown or disposal of a system.*

	Initiation	Devel/Acquis	Implement	Oper/Maint	Disposal
Applicability		✔		✔	✔✔

Discussion: Although a system may be powered down, critical information still resides on the system and could be retrieved by an unauthorized user or organization. Access to critical information systems must be controlled at all times.

At the end of a system's life-cycle, system designers should develop procedures to dispose of an information system's assets in a proper and secure fashion. Procedures must be implemented to ensure system hard drives, volatile memory, and other media are purged to an acceptable level and do not retain residual information.

4.0 SUMMARY

Now, more than ever, IT security is a critical element in the system life cycle. Security must be incorporated and addressed from the initial planning and design phases to disposal of the system. Without proper attention to security, one of an organization's most valuable asset—its information—is subject to loss. With careful planning from the earliest stages, however, security becomes an enabler, and supports the organization in achieving its mission.

As security awareness becomes a way of life within an organization, people at all levels, and roles in the system life cycle, should have access to easily-understood guidance. From users to system administrators and program managers, everyone should have a basic understanding of the security principles governing the system they are using, maintaining, or designing and developing.

This document provides a starting point. The principles contained herein are derived from a number of national and international documents, as well as from the experience of the scientists at NIST. It is hoped that these principles will contribute to improved IT security in any organization.

APPENDIX A–IT SPECIALIST POSITIONS

Within the Federal Government the Office of Personnel Management (OPM) has recently created an Information Technology Management series occupation title of Information Technology Specialist. Within the IT Specialist occupation OPM has identified several specialty areas referred to as "parenthetical titles" that are added to the basic occupational title. OPM created these titles in an effort to assist in determining what type of occupational skills are needed to properly address systems security issues during the system life cycle and to achieve some degree of standardization in referring to those who play key roles in systems security. The parenthetical titles indicate the types of employees that would have primary action for the systems security efforts during systems development. Skill levels will vary by individual so assignment of an employee to a specific task is a management decision.

The table below relates the skills and knowledge found in a given specialty area to the systems security role within a given phase of the system life cycle development process. This information is provided so that organizations can address the appropriate engineering principles in the roles and responsibilities section of organizations' system IT life-cycle policies, employee performance plans, and in the required duties section of position descriptions. It is noted that within a given organization, roles may differ from this list of specialties.

Specialty Area	**System Development Life Cycle Phase**				
	Initiation	**Development/ Acquisition**	**Implement**	**Operation & Maintenance**	**Disposal**
Customer Support Specialty	✓	✓	✓✓	✓✓	✓✓
Data Management Specialty	✓✓	✓✓	✓	✓	
Information Systems Security Specialty	✓✓	✓✓	✓✓	✓	✓
Internet Specialty	✓	✓✓	✓✓	✓✓	
Network Services Specialty	✓	✓✓	✓✓	✓✓	
Policy, Planning and Management Specialty	✓✓	✓✓	✓	✓	✓
Software Engineering, Applications Specialty		✓✓	✓✓	✓	✓
Software Engineering, Systems Specialty	✓✓	✓✓	✓✓	✓	✓
System Administration Specialty			✓✓	✓✓	✓✓
Systems Analysis Specialty	✓✓	✓✓	✓	✓	✓

APPENDIX B–DEFINITIONS

Term	Definition
access control	Enable authorized use of a resource while preventing unauthorized use or use in an unauthorized manner.
accountability	The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.
assurance	Grounds for confidence that the other four security goals (integrity, availability, confidentiality, and accountability) have been adequately met by a specific implementation. "Adequately met" includes (1) functionality that performs correctly, (2) sufficient protection against unintentional errors (by users or software), and (3) sufficient resistance to intentional penetration or by-pass.
authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.
authorization	The granting or denying of access rights to a user, program, or process.
availability	The security goal that generates the requirement for protection against intentional or accidental attempts to (1) perform unauthorized deletion of data or (2) otherwise cause a denial of service or data.
confidentiality	The security goal that generates the requirement for protection from intentional or accidental attempts to perform unauthorized data reads. Confidentiality covers data in storage, during processing, and while in transit.
data integrity	The property that data has not been altered in an unauthorized manner. Data integrity covers data in storage, during processing, and while in transit.
denial of service	The prevention of authorized access to resources or the delaying of time-critical operations. (time-critical may be milliseconds or it may be hours, depending upon the service provided.)
domain	See security domain.

entity	Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information).
general support system	An interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.
integrity	The security goal that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).
identity	Information that is unique within a security domain and which is recognized as denoting a particular entity within that domain.
IT-related risk	The net mission/business impact considering (1) the probability that a particular threat source will exploit, or trigger, a particular information system vulnerability and (2) the resulting impact if this should occur. IT related-risks arise from legal liability or mission/business loss due to: 1. Unauthorized (malicious, non-malicious, or accidental) disclosure, modification, or destruction of information. 2. Non-malicious errors and omissions. 3. IT disruptions due to natural or man-made disasters. 4. Failure to exercise due care and diligence in the implementation and operation of the IT.
IT security architecture	A description of security principles and an overall approach for complying with the principles that drive the system design; i.e., guidelines on the placement and implementation of specific security services within various distributed computing environments.
IT security goal	See “Security goal.”

major application	An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.
object	A passive entity that contains or receives information. Note that access to an object potentially implies access to the information it contains.
risk	Within this document, synonymous with "IT-related risk."
risk analysis	The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.
risk assessment	See risk analysis
risk management	The ongoing process of assessing the risk to mission/business as part of a risk-based approach used to determin adequate security for a system by analyzing the threats and vulnerabilities and selecting appropriate, cost-effective controls to achieve an maintain an acceptable level or risk.
security	Security is a system property. Security is much more that a set of functions and mechanisms. IT security is a system characteristic as well as a set of mechanisms which span the system both logically and physically.
security domain	A set of subjects, their information objects, and a common security policy.
security policy	The statement of required protection of the information objects.
security goals	The five security goals are confidentiality, availability, integrity, accountability, and assurance.
security service	A capability that supports one, or many, of the security goals. Examples of security services are key management, access control, and authentication.
subject	An active entity, generally in the form of a person, process, or device, that causes information to flow among objects or changes the system state.

system integrity	The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.
threat	Any circumstance or event with the potential to harm an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service.
threat source	Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) the situation and method that may accidentally trigger a vulnerability.
threat analysis	The examination of threat sources against system vulnerabilities to determine the threats for a particular system in a particular operational environment.
vulnerability	A weakness in system security requirements, design, implementation, or operation, that could be accidentally triggered or intentionally exploited and result in a violation of the system's security policy.

APPENDIX C – REFERENCES

Management of Federal Information Resources, Circular A-130, Office of Management and Budget (OMB). http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html

Common Criteria for Information Technology Security Evaluation (CC), Version 2.1, August 1999. http://www.commoncriteria.org/

Generally Accepted Principles and Practices for Securing Information Technology Systems, SP 800-14, National Institute of Standards and Technology, September 1996. http://csrc.nist.gov/publications/nistpubs/index.html

Guide for Developing Security Plans for Information Technology Systems, SP 800-18, National Institute of Standards and Technology, December 1998. http://csrc.nist.gov/publications/nistpubs/index.html

Information Assurance Technical Framework (IATF), Release 3.0, October 2000. http://www.iatf.net/, member-only area, site registration at: https://www.iatf.net/register/

Job Family Position Classification Standard for Administrative Work in the Information Technology Group Series (Draft), GS-2200A, Office of Personnel Management. http://www.opm.gov/fedclass/html/draft.htm

NSTISSI No. 4009, *National Information Systems Security (INFOSEC) Glossary*, (Revision 1), January 1999. http://www.nstissc.gov/Assets/pdf/4009.pdf. While the majority of NSTISSI-4009 definitions are used, some of the definitions in Appendix B have been determined to be more appropriate to the task of defining a technical baseline for IT security than similar definitions in NSTISSI-4009.